# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/943,858 | 08/30/2001 | Ichiro Futamura | 09792909-5128 | 2227 |

26263 7590 03/23/2005

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

| EXAMINER | |
|---|---|
| ELMORE, JOHN E | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | |

DATE MAILED: 03/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/943,858 | FUTAMURA ET AL. | |
| | Examiner | Art Unit | |
| | John Elmore | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *30 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-24 and 26-29* is/are rejected.

7)☒ Claim(s) *11 and 25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-29 have been examined.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 1, 4, 15, 28 and 29 are rejected under 35 U.S.C. 102(b)** as being anticipated by Yu et al., hereafter Yu (US 5,930,804).

**Regarding claim 1**, Yu discloses a person authentication system comprising:

a person identification authority (authorization center 24) for creating a person identification certificate storing the template (col. 6, lines 42-46; col. 9, lines 12-17 and 61-64; col. 10, lines 3-8);

an entity which executes person authentication (authorization center 24 containing biometric server 42) for comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate (col. 11, lines 5-13); and

an entity (web server 30 on web server section 20) which requests person authentication for requesting to said entity which executes person authentication for person authentication (col. 7, lines 64-66).

**Regarding claim 4**, Yu teaches all the limitations of claim 1, and further teaches a system wherein

said entity which requests person authentication is a user device or a service provider (web server 30 on web server section 20 as service provider), and

said entity which executes person authentication is said person identification authority (authorization center 24 containing biometric server 42), and

said user device or said service provider provides the sampling information input by a user to said person identification authority (web client 17 on web client section 14 as user device provides authorization center 24 with biometric data; col. 6, lines 21-23 and 42-46; col. 17, lines 45-46),

whereby said person identification authority decrypts the template that has been encrypted in the person identification certificate by using a private key of said person identification authority (digital signature; col. 18, lines 24-27)

and compares the decrypted template with the sampling information input by a user provided from said user device or said service provider, thereby performing person authentication (col. 8, lines 9-21, and col. 11, lines 5-13).

**Regarding claims 15 and 18**, these are a method version of the claimed system discussed above (claims 1 and 4), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

**Regarding claim 29**, this a program-providing-medium version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

3. **Claim 1, 15 and 29 are rejected under 35 U.S.C. 102(e)** as being anticipated by Dulude et al., hereafter Dulude (US 6,310,966).

Dulude discloses a person authentication system comprising:

a person identification authority for creating a person identification certificate storing the template (registration authority 34; Fig. 3; col. 4, lines 12-19);

an entity which executes person authentication for comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate (receiving section 42; col. 7, lines 33-44); and

an entity which requests person authentication for requesting to said entity which executes person authentication for person authentication (input devices 44 and 48; col. 5, lines 50-62, and col. 8, lines 1-4).

**Regarding claim 15**, this a method version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

**Regarding claim 29**, this a program-providing-medium version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

4. **Claims 1, 2, 13, 15, 16, 27 and 29 are rejected under 35 U.S.C. 102(e)** as being anticipated by Bianco et al., hereafter Bianco (US 6,256,737).

**Regarding claim 1**, Bianco discloses a person authentication system comprising:

a person identification authority for creating a person identification certificate storing the template (public key system engine 2902; col. 56, lines 40-44);

an entity which executes person authentication for comparing the template with the sampling information input by a user as person authentication on the basis of the person identification certificate (computer 208 executes authentication via internal authentication object 720; Fig. 7; Fig. 8A-1 steps 816-820; col. 24, lines 21-37, and col. 56, lines 58-65 (use of digital signature)); and

an entity which requests person authentication for requesting to said entity which executes person authentication for person authentication (computer 208 requests authentication; col. 12, lines 18-22).

**Regarding claim 2**, Bianco teaches all the limitations of claim 1, and further teaches a system wherein

said entity which requests person authentication and said entity which executes person authentication are included in a user device serving as a data processing apparatus having the comparison/verification capability (computer 208 includes biometric device object 722 which compares templates; col. 24, lines 21-43),

and said person identification authority provides the person identification certificate storing the template that has been encrypted by a public key of said user

device, whereby said user device decrypts the encrypted template in the received person identification certificate by using a private key of said user device, and compares the decrypted template with the sampling information input by a user, thereby performing person authentication (biometric server 104 sends template encrypted with receiver's public key to computer 208 for comparison; col. 24, lines 21-31, and col. 56, lines 49-65).

**Regarding claim 13**, Bianco teaches all the limitations of claim 1, and further teaches that

said entity which executes person authentication is a user device (computer 208 containing biometric device object 722; col. 24, lines 21-43), and

said entity which requests person authentication is a service provider for providing service to said user device (web server 212; col. 12, lines 25-36), and

the said user device decrypts, by using a private key of said user device, the template that has been encrypted in the person identification certificate received from said person identification authority (col. 55, lines 28-35. and col. 56, lines 62-65) and

compares the template with the sampling information input by a user, thereby performing person authentication and notifying said service provider of the result of comparison (col. 24, lines 35-43).

**Regarding claims 15, 16 and 27**, these are a method version of the claimed system discussed above (claims 1, 2 and 13), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also are anticipated.

**Regarding claim 29**, this a program-providing-medium version of the claimed system discussed above (claim 1), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also is anticipated.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 3, 7, 8, 10 and 12 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Dulude in view of Bianco et al., hereafter Bianco (US 6,256,737).

**Regarding claim 3,** Dulude teaches all the limitations of claim 1, and further teaches the system wherein

said entity which requests person authentication is a user device (transmitting section 40; col. 5, lines 50-62, and col. 8, lines 1-4), and

said entity which executes person authentication is a service provider (reception section 42) for providing service to said user device (col. 4, lines 19-25), and

said person identification authority (registration authority 34) provides the person identification certificate (biometric certificate) storing the template (registration biometric data),

whereby said user device provides the sampling information input (transaction biometric data) by a user to said service provider (col. 5, lines 63-67), and

said service provider compares the template with the sampling information input by a user provided from said user device, thereby performing person authentication (col. 7, lines 33-44).

But Dulude does not explain that said person identification authority encrypts the template with the public key of said service provider and that said service provider decrypts the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider.

However, Bianco teaches a system wherein a person identification authority (biometric registration authority 34) encrypts a template (registration biometric data) with the public key of a service provider and that said service provider decrypts the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider (col. 55, lines 30-35, and col. 56, lines 40-65) for the purpose of establishing a more trustworthy networking environment (col. 55, lines 43-57).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Bianco to include the encryption of the template with the public key of said service provider and the subsequent decryption by said service provider of the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider. One would be motivated to do so in order to establish a more trustworthy networking environment.

**Regarding claim 7**, Dulude teaches all the limitations of claim 1, and further teaches a system comprising:

a mobile terminal storing certificate (smart card of the user; col. 5, lines 45-49),

the person identification wherein said entity which executes person authentication receives, from said mobile terminal, the person identification certificate and a key for encrypting and decrypting the template of the person identification certificate (col. 6, lines 32-35 and 62-65), and

decrypts the template stored in the received person identification certificate by using the key for encrypting and decrypting the template, thereby performing person authentication (col. 6, lines 61-62).

Although Dulude teaches that biometric data transmitted over a network between the transmitting section 24 and the receiving section 42 is encrypted (col. 5, lines 63-67) and that the memory storing the template is accessed by the biometric certificate extractor 64 over a network (col. 5, lines 32-41), Dulude does not explicitly explain that the key for encrypting and decrypting the template of the person identification certificate is decrypted first by using a private key of said mobile terminal.

However, Bianco teaches a system wherein all biometric templates transmitted over the network to and from the person identification authority (biometric server 104) are encrypted using a public-key/private-key system (col. 56, lines 62-65) for the purpose of establishing a more trustworthy networking environment (col. 55, lines 30-57). Further, one of ordinary skill in the computer art at the time the invention was made would recognize that the decryption of a template by the mobile terminal using the

private key of the mobile terminal means that the encryption was not the digital signature of the mobile terminal and, hence, was not a means by the mobile terminal of verifying the template; rather, it followed as a consequence of receiving the template from the person identification authority, which encrypted it (along with the digital signature of the authority) with the public key of the mobile terminal prior to transmitting it over the network.

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Bianco such that the key for encrypting and decrypting the template of the person identification certificate is decrypted first by using a private key of said mobile terminal. One would be motivated to do so in order to establish a more trustworthy networking environment.

**Regarding claim 8**, all its limitations have been addressed by the modified invention of Dulude and Bianco in claim 7. Thus, for the reasons provided above, such a claim also would have been obvious.

**Regarding claim 10**, Dulude teaches all the limitations of claim 1, and further teaches that

said entity which requests person authentication is a user device (devices 44 and 48 and smart card 66; col. 5, lines 33-62), and

said entity which executes person authentication is a service provider for providing service to said user device (receiving section 42; col. 8, lines 34-45, which incorporates by reference Vaeth, US 6,035,402; see Veath, col. 6, lines 5-26), and

said user device provides the sampling information input by a user (col. 5, lines 63-67) and the person identification certificate storing the template (biometric certificate stored in smart card of the user), and

compares the template with the sampling information input by a user provided from said user device, thereby performing person authentication (col. 7, 33-44).

But Dulude does not explain that said service provider decrypts, by using a private key of said service provider, the template that has been encrypted in the person identification certificate.

However, Bianco teaches a system wherein a person identification authority (biometric registration authority 34) encrypts a template (registration biometric data) with the public key of a service provider and that said service provider decrypts the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider (col. 55, lines 30-35, and col. 56, lines 40-65) for the purpose of establishing a more trustworthy networking environment (col. 55, lines 43-57).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Bianco to include the encryption of the template with the public key of said service provider and the subsequent decryption by said service provider of the encrypted template in the person identification certificate received from said person identification authority by using a private key of said service provider. One would be motivated to do so in order to establish a more trustworthy networking environment.

**Regarding claim 12**, Dulude teaches all the limitations of claim 1, and further teaches that

said entity which requests person authentication is a user device (devices 44 and 48 and smart card of the user 68), and

said entity which executes person authentication is a service provider for providing service to said user device (receiver section 42; col. 8, lines 34-45 incorporating by reference Vaeth; see Vaeth, col. 6, lines 5-26), and

said service provider receives the template in the person identification certificate from said user device, thereby performing person authentication on the basis of the received template (col. 6, lines 32-34, and col. 7, lines 33-44).

But Duluth does not explain that the template has been decrypted by using a private key of said user device prior to sending the template to the service provider.

However, Bianco teaches a system wherein all biometric templates transmitted over the network to and from the person identification authority (biometric server 104) are encrypted using a public-key/private-key system (col. 56, lines 62-65) for the purpose of establishing a more trustworthy networking environment (col. 55, lines 30-57). Further, one of ordinary skill in the computer art at the time the invention was made would recognize that the decryption of a template by user device using the private key of the user device means that the encryption was not the digital signature of the user device and, hence, was not a means by the user device of verifying the template; rather, it followed as a consequence of receiving the template from the person

identification authority which encrypted it (along with the digital signature of the authority) with the public key of the user device prior to transmitting it over the network.

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Bianco such that that the template encrypted by the person identification authority using the public key of the user device prior to sending the template to the user device for storage and is subsequently decrypted by using the private key of said user device prior to sending the template to the service provider. One would be motivated to do so in order to allow the use of establish a more trustworthy networking environment.

**Regarding claims 17, 21, 22, 24 and 26**, these are a method version of the claimed system discussed above (claims 3, 7, 8, 10 and 12), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

6. **Claims 5 and 6 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Bianco in view of Dulude.

**Regarding claim 5**, Bianco teaches all the limitations of claim 1, and further teaches a system wherein said person identification authority (biometric server 104) encrypts the template by using a public key of said entity which executes person authentication and stores the encrypted template in the person identification certificate, thereby transmitting the stored template to said entity which executes person authentication (col. 24, lines 21-31; col. 55, lines 30-35; col. 56, lines 62-64).

Although Bianco teaches the use of digital signatures in authenticating data sent between entities (col. 54, lines 28-32; col. 56, lines 40-44 and 62-65), Bianco does not explicitly explain that the person identification authority decrypts the template that has been encrypted and stored in the person identification certificate by using a private key of said person identification authority prior to re-encrypting the template and transmitting it to said entity.

However, Dulude teaches a biometric authentication system wherein a person identification authority (registration authority 34) encrypts the template with its private key (creating a digital signature) prior to storing the template in memory (col. 4, lines 12-19 and 61-65; Fig. 2) for the purpose of providing an entity which retrieves the template from memory with a means of verifying the template's authenticity (col. 6, lines 59-62). One of ordinary skill in the computer art would recognize that where the person identification authority itself retrieves the template from memory prior to transmitting it to another entity, verification of the template requires that the authority first use its own public key to decrypt the template.

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Bianco with the teaching of Dulude such that said person identification authority decrypts the template that has been encrypted and stored in the person identification certificate by using a private key of said person identification authority prior to encrypting the template and transmitting it. One would be motivated to do so in order to verify the authenticity of the stored template prior to transmitting it.

**Regarding claim 6**, it is the same as the modified invention of Bianco and Duluth in claim 5 but with an additional limitation. As such, Bianco further teaches that said person identification authority receives a public key certificate from said entity, which executes person authentication and reads a public key after verifying the public key certificate (col. 23, lines 38-40; col. 54, lines 28-32; col. 56, lines 62-65). Therefore, for reasons provided here and above in claim 5, such a claim also would have been obvious.

**Regarding claims 19 and 20**, these are a method version of the claimed system discussed above (claims 5 and 6), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such claims also would have been obvious.

7. **Claim 9 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Dulude in view of Bianco and further in view of Praca et al. hereafter Praca ("From Smart Cards to Smart Objects," Gemplus Developer Conference 2000 white paper, June 2000).

Dulude teaches all the limitations of claim 1, and further teaches a system comprising:

a mobile terminal storing the person identification certificate (smart card of the user; col. 5, lines 45-49),

wherein said entity which executes person authentication (receiving section 42) decrypts the template that has been encrypted in the person identification certificate stored in said mobile terminal (col. 6, lines 58-65) and

compares the decrypted template with the sampling information input by a user, thereby performing person authentication (col. 7, lines 33-44).

But Dulude does not explain that the entity which executes person authentication is the mobile terminal and that said mobile terminal decrypts, by using a private key of said mobile terminal, the template that has been encrypted in the person identification certificate stored in said mobile terminal.

However, Praca teaches an authentication system wherein the entity which executes personal authentication is a mobile terminal (smart card) for the purpose of providing a more secure means of authentication by not having to rely on an external process decision that could be compromised (page 4, paragraphs 1 and 2). Further, Bianco teaches a system wherein all biometric templates transmitted over the network to and from the person identification authority (biometric server 104) are encrypted using a two-key system (col. 56, lines 62-65) for the purpose of establishing a more trustworthy networking environment (col. 55, lines 30-57). And one of ordinary skill in the computer art at the time the invention was made would recognize that the decryption of a template by the mobile terminal using the private key of the mobile terminal means that the encryption was not the digital signature of the mobile terminal and, hence, was not a means by the mobile terminal of verifying the template; rather, it followed as a consequence of receiving the template from the person identification authority, which encrypted it (along with the digital signature of the authority) with the public key of the mobile terminal prior to transmitting it over the network.

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teachings of Bianco and Praca such that the entity which executes is the mobile terminal and the key for encrypting and decrypting the template of the person identification certificate is decrypted first by using a private key of said mobile terminal. One would be motivated to do so in order to establish a more secure authentication scheme and trustworthy networking environment.

**Regarding claim 23**, this is a method version of the claimed system discussed above (claim 9), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also would have been obvious.

8. **Claim 14 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Dulude in view of Yu.

Duluth teaches all the limitations of claim 1, and further teaches a system wherein data is transmitted together with a digital signature that is verified, so as to check whether the data has been tampered with or not in mutual data communication performed by said person identification authority, said entity which executes person authentication and said entity which requests person authentication (digital signature 22; Fig. 2; col. 4, lines 55-65).

But Duluth does not explain that mutual authentication is performed between data transmission devices.

However, Yu teaches a biometric authentication system wherein mutual authentication is performed between data transmission devices (SSL provides mutual authentication; col. 4, lines 54-67; col. 6, lines 42-46; col. 8, lines 27-29; col. 12, lines 51-57) for the purpose of providing secure transport of data that includes server authentication (col. 12, lines 51-57).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teachings of Yu such that mutual authentication is performed between data transmission devices. One would be motivated to do so in order to provide the secure transport of data that includes server authentication in a client-server system.

**Regarding claim 28**, this is a method version of the claimed system discussed above (claim 14), wherein all claim limitations have been addressed. Thus, for the reasons provided above, such a claim also would have been obvious.

### *Allowable Subject Matter*

9. **Claims 11 and 25 are objected to** as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

**Regarding claim 11**, Duluth, the closest prior art, teaches that the service provider (receiver section 42) receives the biometric certificate 68 from the user device

(devices 44 and 48 and smart card of the user 68) and that the service provider decrypts the template (biometric data) in the certificate (col. 7, lines 33-44).

But Duluth does not explain that said service provider transmits the result of verifying a signature of said person identification authority written in the person identification certificate provided by said user device to said user device and transmits the result of verification to said user device, and that the user device then provides to the service provider the decrypted key with which to decrypt the template enclosed with the biometric certificate along with the sampling information on condition that the signature is verified to have never been tampered with.

No known prior art teaches a service provider that receives from a user device a key for decrypting data contained within a certificate only upon the report by the service provider of the successful verification of the attached digital signature of the authority that created the certificate. Therefore, it would not have been obvious to one of ordinary skill in the computer art at the time the invention was made to modify the invention of Duluth accommodate the limitations of claim 11.

**Regarding claim 15**, this is a method version of the claimed system discussed above (claim 11) and would be allowable for the same reasons as provided above.

***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cordery et al. (US 5,796,841) teaches a system for authentication of users for e-

commerce involving digital certificates.

Deo et al. (US 5721781) teaches a system for mutual authentication of entities over a network by exchanging digital signatures.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100